January 23, 2003

The Honorable John Warner
Chairman
Senate Committee on Armed Services
228 Russell Senate Office Building
Washington, DC 20510
The Honorable Carl Levin
Senate Committee on Armed Services
228 Russell Senate Office Building
Washington, DC 20510

Dear Chairman Warner and Senator Levin:

On behalf of USACM, the Association for Computing Machinery's U.S. Public Policy Committee, we are writing to express some concerns regarding the Total Information Awareness (TIA) Program, sponsored by the Department of Defense. We share the nation's desire to improve security against terrorist acts, and we acknowledge that significant contributions can be made to public safety and national defense with advances in computing technology.

Research into areas such as new data mining and fusion methods and privacy-enhancement technologies is needed and welcomed. However, the overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. Technological research alone cannot make a system such as TIA viable.

As computer scientists and engineers we have significant doubts that the computer-based TIA Program will achieve its stated goal of "countering terrorism through prevention". Further, we believe that the vast amount of information and misinformation collected by any system resulting from this program is likely to be misused to the detriment of many innocent American citizens.

Because of serious security, privacy, economic, and personal risks associated with the development of a vast database surveillance system, we recommend a rigorous, independent review of these aspects of TIA. Such a review should include an examination of the technical feasibility and practical reality of the entire program. USACM would be pleased to assist in such an effort.

Security Risks.

Immense databases, such as are being proposed by TIA - whether operated by governmental or commercial organizations - represent substantial security and privacy risks in their own right. An all-encompassing database, compiled from private and governmental databases including financial, medical, educational, telephone, and travel records, will contain large quantities of sensitive information. One or more such databases would provide new targets for exploitation and attack by malicious computer users, criminals, and terrorists. It is unlikely that sufficiently robust databases of the

required size and complexity, whether centralized or distributed, can be constructed, financed, and effectively employed in a secure environment, even with significant research advances. A single individual who has a personal or political vendetta, or who has been compromised by blackmail or greed, could do great harm. Yet, tens of thousands of systems administrators, domestic law enforcement staff, and intelligence personnel will be able to access the data; the security of the data will depend on the trustworthiness of every one of them. This is not something that can be guaranteed with technology.

The databases proposed by TIA also would increase the risk of identity theft by providing a wealth of personal information to anyone accessing the databases. A recent case of massive identity theft involved a computer help-desk employee who abused his access to sensitive passwords from banks and credit companies to obtain personal information on over 30,000 people over a period of three years. The employee then sold the personal information to a number of scam artists. Imagine how much more damage could be done with a database as comprehensive as that envisioned by those who support the TIA. Imagine how effective a terrorist organization could be if it could use those to pass themselves off as trustworthy citizens who hold security clearances.

Privacy Risks.

Privacy is a fundamental American value. Fair Information Practices were developed because policymakers recognized that there are critical issues of privacy when aggregating data that was collected for other purposes. First formulated by a Department of Health, Education and Welfare committee in 1973, the Code of Fair Information Practices is the foundation for the federal Privacy Act of 1974 and the privacy laws of the country. It prohibits secret databases and mandates fairness, accountability, and due process for individuals about whom information is gathered. The need for oversight and control is especially great when aggregation and analysis of personal information is done without the knowledge or consent of the people being monitored.

It is misleading to suggest that "privacy enhancing technologies" within TIA can protect people's privacy, because by definition surveillance compromises privacy. Furthermore, the secrecy inherent in TIA implies that citizens could not verify that information about them is accurate and shielded from misuse. Worse yet would be the resulting lack of protection against harassment or blackmail by individuals who have inappropriately obtained access to an individual's information, or by government agencies that misuse their authority. Again, these are concerns that cannot be completely addressed, even with advances in technology.

Economic Risks.

The success of electronic commerce in the U.S. may be threatened by TIA. Independent research has repeatedly shown that ensuring confidence in privacy preservation is fundamental to the continued growth of electronic commerce, a technology in which the U.S. is preeminent and on which a significant part of our future economic growth depends. In addition, as most non-Americans would oppose allowing the U.S. government to access private information about them, we could expect the development of e-commerce systems that exclude the U.S., thereby depriving American companies of

significant export opportunities. For example, a European Union subsidiary of a U.S. based e-commerce company might be forbidden from running the company's systems in the EU because of the EU's Data Privacy Directive. Alternatively, if privacy restrictions elsewhere in the world conflict with TIA-inspired surveillance, companies may be forced to develop and operate expensive, parallel systems of record-keeping for non-U.S. customers.

Finally, the cost of identity theft to businesses, government, and victims is significant and increasing. National bank regulators approximated half a million cases of identity theft a year. Costs due to identity theft are currently estimated to be in the billions of dollars. Not only will all these stolen identities introduce "noise" into the TIA database, the potential for more significant theft via this aggregated database system could greatly magnify the total costs to citizens, businesses, and government.

Personal Risks.

Because TIA would combine some types of automated data-mining with statistical analysis, there would be a significant personal cost for many Americans. Any type of statistical analysis inevitably results in some number of false positives - in this case incorrectly labeling someone as a potential terrorist. As the entire population would be subjected to TIA surveillance, even a small percentage of false positives would result in a large number of law-abiding Americans being mistakenly labeled.

For example, suppose the system has an 99.9% accuracy rate. We believe that having only 0.1% of records being misclassified as belonging to potential terrorists would be an unachievable goal in practice. However, if records for everyone in the U.S. were processed monthly, even this unlikely low rate of false positives could result in as many as 3 million citizens being wrongly identified each year. More realistic assumptions about the percentage of false positives would drive the number even higher. Research to increase accuracy and eliminate false positives in such systems is clearly worthwhile, but the rate can never be reduced to zero while maintaining some functionality. Is any level of false positive acceptable - and Constitutional - in such a system?

The existence of TIA would impact the behavior of both real terrorists and law-abiding individuals. Real terrorists are likely to go to great lengths to make certain that their behavior is statistically "normal," and ordinary people are likely to avoid perfectly lawful behavior out of fear of being labeled "Un-American."

To summarize, we appreciate that the stated goal of TIA is to fund research into new technologies and algorithms that could be used in a large surveillance system in the service of eliminating terrorist acts. However, we are extremely concerned that the program has been initiated and some projects already funded apparently without independent oversight and without sufficient thought being given to real constraints - technical, legal, economic, and ethical - on project scope, development, field testing, deployment, and use. Consequently, the deployment of TIA, as we currently understand it, would create new risks while having an unknown effect on overall security.

There are important steps that the government can take now to increase our security without creating a massive surveillance program that has the potential of doing more harm than good. Federal, state and local governments already have information

systems in place that could play major roles with highly focused "terrorist spotting". However, many of these information systems are only partly functional and/or being ineffectively used. An example is the computer system run by the Federal Bureau of Alcohol, Tobacco and Firearms which, according to the New York Times, was unable to link bullets fired in three sniper shootings in Maryland and Georgia in September, 2002. Serious improvements in the use of current operational systems could significantly enhance homeland security without creating the major new risks noted in this letter. We would be very pleased to assist policymakers in those efforts, especially as they relate to reducing the risk of attacks on our information infrastructure.

Please contact the ACM Office of Public Policy Office at (202) 478-6312 if we can be of assistance.

Sincerely,

Barbara Simons, Ph.D.
Eugene H. Spafford, Ph.D
Co-Chairs
U.S. ACM Public Policy Committee
Association for Computing Machinery

About USACM:

USACM is the U.S. Public Policy Committee of the Association for Computing Machinery (ACM). ACM is the leading nonprofit membership organization of computer scientists and information technology professionals dedicated to advancing the art, science, engineering and application of information technology. Since 1947, ACM has been a pioneering force in fostering the open interchange of information and promoting both technical and ethical excellence in computing. Over 70,000 computer scientists and information technology professionals from around the world are members of ACM.